Plan d'Assurance Qualité des projets Publik gérés par Entr'ouvert
Plan d'Assurance Sécurité de la plate-forme Publik gérée par Entr'ouvert

Version octobre 2018
Version originale disponible sur : https://dev.entrouvert.org/projects/publik/wiki/PAQ-PAS

Plan d'Assurance Qualité

Environnement du projet

Présentation et but du projet client

Le projet de [...], [...] habitants, a pour objectif la mise en place d'une solution de Gestion de la Relation Citoyen. La solution doit permettre d'atteindre concomitamment trois grands objectifs :

- Simplifier la vie des citoyens en leur permettant d'accomplir les démarches à tout moment sans se déplacer.
- Simplifier le travail des agents en les débarrassant des tâches répétitives.
- Ouvrir le système d'information de la collectivité en permettant aux différentes applications métiers de communiquer.

Équipe Entr'ouvert

L'équipe projet Entr'ouvert est composée des personnes suivantes :

- Mikaël Ates : chef de projet fonctionnel, consultant, expert gestion d'identités, ingénieur de recherche.
- Emmanuel Cazenave : chef de projet technique, développeur.
- Victor Claudet : chef de projet fonctionnel, consultant, expert e-administration.
- Pierre Cros : chef de projet fonctionnel, consultant, expert e-administration.
- Benjamin Dauvergne : chef de projet technique, expert gestion d'identités, développeur.
- Josué Kouka : chef de projet technique, développeur.
- Stéphane Laget : chef de projet fonctionnel, consultant, expert e-administration.
- Brice Mallet : chef de projet fonctionnel, consultant, expert e-administration.
- Serghei Mihai : chef de projet technique, développeur.
- Thomas Noël : administrateur système et réseau, chef de projet technique, développeur.
- Frédéric Péters : chef de projet technique, développeur.
- Christophe Siraut : administrateur système, développeur.
- et Paul Marillonet : doctorant CIFRE.
  Cette équipe représente la maîtrise d'œuvre (MOE).

Rôles

Voici les rôles qui sont attribués aux membres de l'équipe :

- Chef de projet & Responsable qualité : [...]
  - Coordonne l'équipe projet et les tâches de chacun ;
  - Veille au bon déroulement du projet ;
  - Responsable des formations fonctionnelles ;
  - Veille au respect des règles de qualité.
- Responsable développement : [...]
  - Prend en charge l'environnement de développement ;
  - Responsable des formations techniques ;
  - Développe une partie du projet.

Coordonnées de l'équipe

Afin de faciliter la communication avec le client, une adresse e-mail unique redirigeant vers les adresses e-mail des membres de l'équipe a été créée : [...]@listes.entrouvert.com. Si besoin les membres de l'équipe sont joignables par messagerie instantanée (protocole jabber/XMPP).
Pour un contact urgent, le chef de projet est disponible dans la mesure du possible pour répondre aux demandes par téléphone.

Lieu de développement

L'équipe projet se trouvera dans les locaux de la société Entr'ouvert et/ou en télé-travail à domicile, joignables en permanence par

mail ou messagerie instantanée. Locaux de la société Entr'ouvert :
Entr'ouvert SCOP ARL
169 rue du Château
75014 Paris
+33 (0)1 43 35 01 35

Site (extranet) projet

Entr'ouvert utilise une forge logicielle (http://dev.entrouvert.org) pour l'ensemble de ses projets depuis sa création.
Pour chaque projet, il est mis à disposition un espace sur cette forge, comprenant :
composition de l'équipe et rôles ;

- le relevé d'actions du projet (activité) ;
- la feuille de route du projet (roadmap) ;
- le suivi des demandes (tickets et risques) concernant le projet ;
- un espace « wiki » ;
- un dépôt de documents ;
- des vues sous force de calendrier, diagramme de gantt ;
- un suivi par mail et/ou flux RSS.
  Le site est accessible à cette adresse : https://dev.entrouvert.org/projects/[...]

Pilotage du projet

Phases

Le projet se découpe en deux phases principales.
En phase 1, seront mis en œuvre des démarches simples, sans connexion avec les applications métiers. Cette phase va permettre aux services de s'approprier la solution, aux directions d'envisager concrètement l'organisation et l'affectation des ressources. Lors de cette phase nous travaillons uniquement sur Publik, sans connecteur. Cela permet de faciliter l'adhésion des services en leur montrant que la solution fonctionne parfaitement et en les préservant des phases de tâtonnement qui existent toujours lorsqu'on l'on fait des connecteurs avec des applications tierces.
Une fois les aspects organisationnels traités, les complexités techniques, essentiellement la connexion aux applications tierces, sont traitées en phase 2. En réalité, les échanges avec les éditeurs, le développement des connecteurs et les tests auront commencé dès le début du projet mais le travail se fera exclusivement sur notre plate-forme de développement pour ne pas perturber la prise en main par les administrateurs fonctionnels et les agents.

Si les phases de réflexion et de modélisation sont un préalable indispensable aux développements proprement dits, nous savons d'expérience que des spécifications pléthoriques ne sont pas la garantie d'une solution adaptée. Il arrive fréquemment que l'on perde en épaisseur de la réalité des usages, ce que l'on gagne en modélisation théorique.
Nous proposons donc un développement itératif : c'est une forme de développement dans laquelle on crée rapidement un prototype de l'application pour le soumettre aux utilisateurs et les autoriser ainsi à préciser ses spécifications. Ceci permet de fournir un prototype plus élaboré, pour converger vers l'application finale. Les projets informatiques ont tendance à se tourner trop tard vers leurs utilisateurs, à un stade du développement où les changements possibles sont souvent d'ordre « cosmétique », ce que nous voulons d'éviter.
Ainsi, le planning de développement sera composé de plusieurs étapes, définies par des jalons qui permettront de voir l'état d'avancement du projet. Ce planning est visible sur le site projet.
Des tests – unitaires et fonctionnels – seront effectués tout au long du développement par l'équipe projet.

Organisation des réunions

À la fin de chaque module de développement ou en fin de phase dans le projet, une réunion jalon sera faite et un compte rendu sera dressé sous format électronique. Ce compte rendu sera disponible pour le client. Le contenu des réunions portera sur :

- le travail achevé à cette date ;
- le travail restant pour le jalon actuel ;
- le travail à fournir pour le prochain jalon ;
- les difficultés rencontrées ;
- la documentation ;
- l'évolution des risques ;
- la mise à jour du planning.
  Chaque responsable fera une synthèse portant sur son domaine.

Livrables

Chaque document et module terminé devra être validé par le client en personne (par compte rendu de réunion validé). La documentation ainsi validée sera immédiatement livrée sous forme électronique via le site projet.

À la fin du projet tous les documents seront consolidés sur le site projet et toutes les sources seront livrées.
Récapitulatif des livrables :

- les codes sources ;
- les documents du projet :
  - le cahier des charges ;
  - la documentation utilisateur ;
  - la documentation technique.

Travail collaboratif

L'équipe projet travaille sur le site projet. Les tickets (demandes) et l'espace « wiki » permettent une grande partie des échanges et sont les outils de base du travail collaboratif.
Le code source est disponible via le site projet et également par le protocole git directement.

Suivi et sauvegarde des documents

Le site projet permet de suivre les modifications apportées aux documents créés via le wiki ou placés sur le dépôt de documents.
Pour les documents créés hors wiki, lors des modifications importantes le rédacteur informera le reste des membres du projet des modifications apportées et demandera le cas échéant une validation de ces modifications.
Le site projet et l'intégralité de ses contenus sont sauvegardés chaque nuit sur une machine hors- site.

Communication

La communication entre l'équipe projet et le client est primordiale pour le bon déroulement du projet. Chaque partie s'engage à répondre à une demande de l'autre sous deux jours ouvrés.
L'équipe projet enverra régulièrement des emails (compte-rendus, jalons) au client pour le tenir informé du déroulement du projet.
Le client doit de son côté intervenir le plus rapidement possible s'il détecte un problème sur le projet.
Après envoi d'un document ou d'une demande de validation au client, l'absence de réponse après 3 jours ouvrés est considérée comme une validation. Toute validation au-delà de ces 3 jours sera traitée comme un risque critique.

Gestion des risques

Méthode

Dès la détection d'un risque qui pourrait compromettre le bon déroulement du projet, l'équipe classe le risque selon deux catégories :

- à surveiller : risque détecté mais qui ne présente pas dans l'immédiat un risque critique ;
- critique : risque qui doit être réglé rapidement car il compromet le bon déroulement du projet (tel que : non respect du planning, impossibilité de finaliser voir de commencer une tâche, etc.)
  Pour chaque risque une fiche sera créée sur le site du projet comme un ticket, qui précisera :
- la nature du risque ;
- sa portée et sa criticité ;
- sa possible résolution.
  En fonction de leur criticité, les fiches risques seront envoyées au chef de projet, au responsable qualité et/ou au responsable développement.

Cycle de vie des fiches

Les fiches risques seront mises à jour au cours de leur résolution ou après une réunion jalon.
De manière exceptionnelle, un risque « à surveiller » peut devenir « critique », et réciproquement, ce qui entraînera la mise à jour de sa fiche risque.
Les « fiches risques » sont placées sur le site projet et font donc partie du plan de sauvegarde général du projet.

Plan d'Assurance Sécurité

Audits de sécurité

Publik a déjà fait l'objet de plusieurs audit de sécurité. Citons ceux conduits par le ministère de l'intérieur et par Montpellier Métropole.
Des audits pourront être réalisés par le maître d'ouvrage ou délégués à un tiers. Le contrôle prendra notamment la forme de tests d'intrusions ou d'audits de code.

Exigences de sécurité concernant les développements

Normalisation du code source

Chaque fichier source commencera par un descriptif de ses fonctionnalités, ainsi que la date de sa conception et l'identité de son créateur.
Chaque fonction commencera par un descriptif de sa ou ses fonctionnalités, ses entrées et ses sorties. Chaque nom de variable sera explicite sur la fonction qu'elle aura dans le programme.
Les codes source respecteront les bonnes pratiques associées au langage concerné, par exemple :

- Python : PEP 8 http://www.python.org/dev/peps/pep-0008/
- C : GNU Coding Standards http://www.gnu.org/prep/standards/standards.html

Utilisation de composants externes

Les composants externes utilisés par l'application seront issus de site réputés fiables, par rapport aux systèmes cibles, aux technologies et aux langages utilisés.
Par exemple :

- systèmes Debian : paquets de Debian stable, éventuellement backports
- langage Python : Python Package Index http://pypi.python.org/pypi (paquets de niveau 5)
- framework Django : applications maintenues de http://djangopackages.com/

Tests des sources

Des tests unitaires seront fournis pour les parties jugées les plus risquées du code, et notamment sur les APIs. Les tests fonctionnels sont réalisés si possible en utilisant des framework tels que :

- pour du code Python: unittest (avec intégration dans la documentation via sphinx), nose, coverage
- pour du code C : framework de tests « check » https://libcheck.github.io/check/
  Des tests fonctionnels couvriront l'ensemble des fonctionnalités offertes aux utilisateurs finaux.

Intégration continue

Les tests les plus pertinents sont intégrés à des outils de supervision (nagios) afin de vérifier le fonctionnement permanent de l'application et l'absence de régression.
Ils peuvent aussi faire partie d'étapes de benchmark pour valider des tests de montée en charge.

Procédures d'installation

Les procédures d'installation sont décrites ici :
https://doc-publik.entrouvert.com/guide-de-l-administrateur-systeme/installation/pre-requis/

Sécurisation des infrastructures

Protection antivirale

Nous appliquons quotidiennement les correctifs de sécurité sur nos serveurs et sur nos postes de travail. Tous les logiciels sont installés et maintenu via des paquets et procédures Debian.

Mises à jour, correctifs de sécurité

Entr'ouvert assure la veille et applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont nous avons la charge et plus particulièrement nous suivons les mise à jour de sécurité du système GNU/Linux Debian.
En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERT-FR (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), le correctif sera appliqué dans un délai de 24 heures sur les infrastructures hébergeant nos logiciels (serveurs, pare-feux, routeurs ouverts vers l'extérieur).
Lorsqu'aucun correctif n'est disponible, nous suivrons les recommandations du CERT-FR dans le cadre d'un contournement provisoire.

Gestion des incidents

L'ouverture d'un incident se fera dès que celui-ci est constaté par Entr'ouvert ou signalé par le Client. Entr'ouvert informera le Client de l'incident dès qu'il le constatera (dans un délai de 1h ouvrée) et établira un premier diagnostic indiquant l'impact (indisponibilité partielle ou totale des services, perte de performances…) avec une durée estimée d'indisponibilité ou de dégradation des services. Entr'ouvert informera le Client de l'état d'avancement du traitement du problème et des mesures prises pour le résoudre.

Entr'ouvert privilégiera la messagerie électronique pour avertir le Client des incidents et des opérations de maintenance éventuelles, n'utilisant d'autres moyens qu'en cas d'urgence.
Le support est dispensé par Entr'ouvert via la plate-forme de dépôt d'incidents, par courriel ou par téléphone de 9h30 à 12h30 et de 14h à 19h, du lundi au vendredi.

Haute disponibilité, plan de continuité d'activité

L'infrastructure de l'hébergement mutualisé de Publik consiste en une série de services répartis sur 3 sites en France (Roubaix, Gravelines et Strasbourg). Les données sont répliquées en continu entre ces sites. En cas de dysfonctionnement d'un site, la continuité du service et l'intégrité des données sont assurées.

Surveillance et contrôle des accès aux locaux

Les serveurs d'Entr'ouvert sont installés dans les data-centers, localisés en France, de la société OVH dont l'accès physique est très contrôlé (uniquement personnel OVH qualifié). La climatisation et la protection électrique sont assurés 24*7.
Une protection contre les attaques DoS et DDoS est intégrée.
Les machines disposent de disques redondés (RAID5) et les disques détectés trop âgés ou commençant à avoir des problèmes sont remplacés sans délais.
Les données de chaque client sont hébergées dans des espaces isolés, notamment dans des bases de données distinctes. Deux instances ne peuvent pas accéder au même données (codes d'accès différents). Les composants logiciels sont isolés dans des machines virtuelles (containers OpenVZ).
L'accès Internet est garanti par OVH avec un taux de disponibilité supérieur à 99,9 %. Sur le matériel comme sur l'accès réseau, OVH garantit un GTI de 1h et GTR de 4h.

Gestion des habilitations

Les comptes administrateurs des machines serveurs sont gérés de façon centralisée via un annuaire et des outils de gestion de configuration. Les connexions et les modifications sont journalisées et surveillées.

Sécurisation des données et des flux

Sauvegardes, restauration et effacement des données

Entr'ouvert gère la sauvegarde de toutes ses installations sur un système hébergé. Nous gardons des sauvegardes quotidiennes sur une période de 3 mois.
Un système d'archivage continu permet de revenir à n'importe quel instant précis de l'état des bases de données.

Confidentialité et intégrité des flux

Les connexions administratives sont réalisées exclusivement via le protocole SSH.

Contrôle et filtrage des flux

Seuls les flux de services web, de connexion postgresql et rabbitmq et de surveillance sont ouverts sur les machines Publik. Les connexions entre serveurs sont limitées à une liste restreinte de machines identifiées.

Exigences de sécurité concernant les personnels

Il n'y a chez Entr'ouvert que du personnel hautement qualifié puisque nous sommes tous pairs (nous possédons tous l'entreprise à parts égales et nous percevons tous le même salaire). Deux personnes s'occupent spécifiquement de l'administration système.

- Christophe Siraut - Administrateur système
  Ingénieur système et réseau depuis 2007, Christophe Siraut a travaillé 10 ans à l'agence fédérale belge pour l'accueil des demandeurs d'asile.

- Thomas Noël - Administrateur réseau, développeur
  Ingénieur Télécom Sud Paris, Thomas Noël est un expert du logiciel libre depuis 1994. Il a travaillé pendant 11 ans à l'Agence universitaire de la Francophonie (organisme qui couvre 50 pays) en tant que responsable des infrastructures technique.

L'ensemble des coopérateurs d'Entr'ouvert sont pleinement conscients des impératifs de sécurité en tant qu'actionnaires et travailleurs au sein de l'entreprise.